

# POLICY AND OBJECTIVES OF THE INTEGRATED MANAGEMENT SYSTEM

## 1. OBJECTIVE, SCOPE AND USERS

The objective of this policy is to establish Panama Digital Gateway's commitment framework to operational excellence, customer satisfaction, information security and regulatory compliance, through an Integrated Management System based on the requirements of the ISO 9001:2015 and ISO 27001:2022 Standards. This policy guides the organization's strategic, operational, and continuous improvement decisions.

This policy applies to **the entire scope of the Information Security Management System (ISMS)**, including:

- The provision of **colocation** services and critical infrastructure for the hosting of information systems for national and international clients, from its Data Center located in Panama City.
- All processes, people, assets and technologies involved in the **operation, support, monitoring, security, continuity and improvement** of such services.
- All relevant stakeholders, including customers, suppliers, regulatory authorities, internal staff, and technology partners.

This policy is owned by the **Chief Executive Officer (CEO)**, who must review and update it at least once a year or when there are significant changes in the ISMS.

Users of this policy are all employees, contractors, and authorized third parties who have access to PDG's information, and other associated assets.

## 2. NORMATIVE REFERENCES

- ISO/IEC 27001 – Requirements 5.2, 6.2 and Control A.5.1.
- ISO 9001:2015 – Requirements 5.2 and 6.2

### 3. RESPONSIBILITIES

ROLE	RESPONSIBILITY
General Management (CEO)	Approving and supporting IMS compliance, allocating resources, and leading by example on quality and safety.
IMS Manager	Coordinate the implementation, maintenance, auditing and improvement of the integrated management system. Ensure compliance with ISO requirements.
Process Managers	Apply IMS requirements in their areas, maintain up-to-date records, implement corrective actions, and promote continuous improvement.
Information Security Officer	Ensure compliance with ISO/IEC 27001, lead risk management, protect information assets, and coordinate incident response.
All staff	Comply with the policies, procedures and controls established in the GIS. Actively participate in training and contribute to continuous improvement.

### 4. INTEGRATED POLICY

At **Panama Digital Gateway** we are committed to excellence, security and continuity in the provision of **colocation** services in our Data Center in Panama, guaranteeing the **high availability, continuity, quality and security** of the infrastructure that supports our customers' information.

To fulfill this commitment:

- We maintain a highly available infrastructure, with technical and organizational controls that guarantee the confidentiality, integrity and availability of information and the continuity of services.
- We comply with applicable legal, regulatory, contractual and normative requirements, as well as with the commitments made to our customers, ensuring traceability, reliability and compliance with service level agreements (SLAs).
- We promote a culture of quality and information security, ensuring that all our staff have safe working conditions, clearly defined roles and continuous training.
- We drive continuous improvement of our processes, services and controls, identifying and managing risks and opportunities that strengthen the sustainability of our business and stakeholder trust.
- We take advantage of Panama's strategic position as a digital hub, generating technological alliances and promoting innovation and digital transformation for the benefit of our clients and society.

In line with this policy, Panama Digital Gateway establishes quality and information security objectives that guide our actions towards continuous improvement, compliance with the commitments made and the generation of trust in our customers and stakeholders. These objectives constitute the practical guide to measure, evaluate and strengthen our organizational performance.

## 5. QUALITY OBJECTIVES

- Guarantee the availability of colocation services to ensure the operational continuity of customers, through 24/7 monitoring of critical infrastructure and the planned execution of preventive maintenance.
- Achieve a level of customer satisfaction equal to or greater than 90% to strengthen trust in PDG, through annual surveys, analysis of results and derived improvement plans.
- Resolve support tickets in a timely manner to meet service level agreements (SLAs), through efficient help desk management and response time tracking.
- Implement at least three continuous improvement initiatives each year to increase the efficiency and quality of services, by identifying opportunities and executing documented optimization projects.

## 6. INFORMATION SECURITY OBJECTIVES

- Protect the confidentiality, integrity and availability of information to safeguard critical customer and PDG assets, through the application of technical, physical and organizational controls aligned with ISO/IEC 27001.
- Effectively manage security incidents to reduce the impact on operations and maintain customer trust, by detecting, logging and responding within a maximum time of 24 hours.
- Comply with 100% of applicable legal, regulatory and contractual requirements to avoid sanctions and reputational risks, through the periodic updating of the legal matrix and compliance verification in internal audits.
- Foster a culture of information security across staff to minimize human risks, through annual training and induction programs that include access procedures, floor rules, and colocation standards.

## 7. COMMUNICATION AND AVAILABILITY

This policy is maintained as documented information and is part of the Integrated Management System (IMS).

It is communicated, understood, and applied at all levels of the organization.

It is available to customers, suppliers, authorities and other relevant stakeholders, as appropriate.

## 8. RECORDS BASED ON THIS DOCUMENT

NAME	LOCATION	RESPONSIBLE	CONTROLS	RETENTION TIME
Annual Plan of Quality and Information Security Objectives		Information Asset Owner	The same as for the protection of information	The list must exist as long as the information itself exists